CYBER SECURITY

IN THE LIGHT OF THE CYBER SECURITY ACT

THE GROWING DEPENDENCE OF ORGANIZATIONS AND SOCIETY AS A WHOLE ON INFORMATION SYSTEMS MAKES INEVITABLE ENSURING OF THEIR SECURITY IN RELATION NOT ONLY TO CYBER THREATS

The growing numbers of information and communication system deployments to support everyday activities has resulted in a similar growth in the dependence of society as a whole on the correct operation of these systems - this situation calls for additional protection of these systems and their data. This is the reason why individual entities (especially organizations) have started to introduce protection from cyber attacks as part of their information security, and why cyber security has become an independent field within information security.

[THE ACT]

The government, represented by the Czech National Security Authority, responded to this development and adopted Act No 181/2014 on cyber security in 2014. This Act covers three areas (called „pillars" in some documents) that are supposed to improve the resilience of information and communication systems to cyber threats and enhance and speed up communication and response in the event of a major cyber threat:

- reporting security incidents to CERTs (both government and national CERTs - Computer Emergency Response Teams) and receiving information about vulnerabilities and ongoing attacks,
- introduction of security measures to protect important information systems and communication or information systems of critical infrastructure, and
- adoption of reactive measures and the establishment of a legislative framework for their enforcement by the Czech NSA.

FEATURES AND BENEFITS

- Compliance with the requirements of the Act and the Directive
- Increase in an organization's readiness for cyber security events or cyber security incidents
- Reduction of risks related to unavailability, leaks or loss of information in information or communication systems
- Optimization of costs of information security assurance based on risk analysis results

Obligations defined in this Act are specifically focused on the following groups of subjects (usually organizations) listed in the order of their estimated frequencies:

- administrators of important information systems,
- administrators of communication or information systems of critical infrastructure,
- entities operating important electronic communication networks.

The above-mentioned definition implies that the impact of this Act on particular entities depends on the characteristics of the operated information or communication systems. These are particularly the following:

- important information systems - i.e. systems matching criteria defined in the Directive (the draft version of this Directive lists basic registers, agenda information systems of basic register editors, ISDS, information systems supporting elements of critical infrastructure that is not critical information infrastructure, information systems of key administrative agencies, information systems providing services and information to the population, etc.),
- communication or information systems of critical infrastructure - i.e. systems defined as such.

The Act defines the following obligations for the above-specified entities:

- designate persons responsible for reporting cyber events to CERTs and for receiving information from CERTS and for taking reactive measures (local CERT/CSIRT organizations; CSIRT - Cyber Security Response Team),
- deliver contact information to CERTS,
- establish an information security management system
- implement security measures at least in the scope defined by the Directive, enhanced with measures arising from the risk analysis results.

The Act and the interrelated legal regulations became valid as of 1 January 2015 with a transition period of 1 year.

[AVAILABLE SERVICES]

ICZ offers the following services to assure an organization's readiness and compliance with the requirements of the Act.

Analysis

As part of this group of services, ICZ provides an IS classification service according to the Cyber Security Act (whether the IS is an important information system, or communication or information system of critical infrastructure) and the IS security status assessment - GAP analysis (identification of the requirements of the Act that the IS complies with and those it does not comply with).

Organization of local CERTs/CSIRTs

ICZ can establish rules for local CERT/CSIRT teams (rules, communication matrix, and personnel for the required positions...)

Security management system establishment/revision

In the field of security management systems, ICZ provides the service of introduction or revision of a current security management system and the performance or updating of a risk analysis. The implementation of these services includes application of the requirements of the Act and the Directive, and adoption of requirements defined in the ISO/IEC 27001:2013 standard.

Security measures proposal

Based on the discovered current state of security measures, the requirements of the Directive and the risk analysis results, ICZ will prepare a proposal for developing new or reviewing current security measures. This proposal will be based on the current situation to the maximum extent, and will take advantage of any existing measures.

Security measures implementation

ICZ offers an implementation service (for both organizational and technical measures) and also consultancy services for the implementation of these measures by traditional suppliers of the customer.

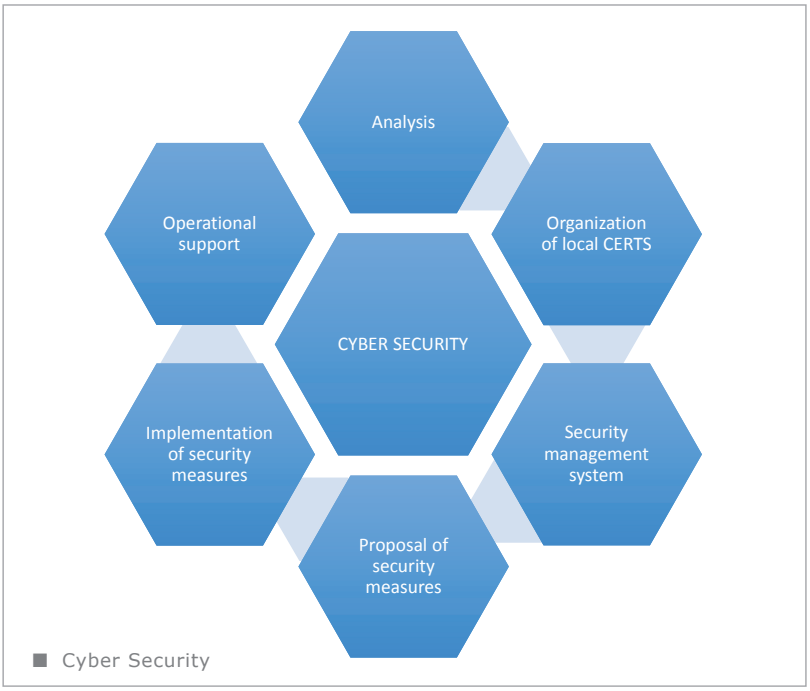
Individual measures can be of several types according to the options and requirements of the customer - from a purely organizational arrangement, through open source tools, to commercial enterprise solutions. ICZ is ready to pay maximum attention to the available options and needs of the customer and provide the relevant measures.

Operational support

Since no security, and especially cyber security, is static, its level must be maintained through a set of activities and processes that together form a security management system. If the customer does not have enough qualified personnel, ICZ can provide training, out-sourcing of selected roles required by the Directive, IS security status assessment (internal IS audit), and entrusted administration or operational support of the implemented technologies.

[FLEXIBILITY]

The above-mentioned services can be combined according to the current needs of the customer.



COMMERCIAL CONTACT

ICZ a.s. Na hrebenech II 1718/10
140 00 Prague 4
TEL.: +420 222 271 111
FAX: +420 222 271 112
E-MAIL: marketing@i.cz